(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 July 2003 (10.07.2003)

PCT

(10) International Publication Number
WO 03/056746 A1

(51) International Patent Classification[7]: H04L 9/08, 29/06

(21) International Application Number: PCT/EP02/00057

(22) International Filing Date: 3 January 2002 (03.01.2002)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET LM ERICSSON (publ)** [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **GOORDEN, Mario** [NL/NL]; Banjostraat 22, NL-4876 XK Etten-Leur (NL). **TAORI, Rakesh** [NL/NL]; Solmsweg 10, NL-5616 CK Eindhoven (NL). **WILLEKENS, Jeroen** [NL/NL]; Annie Romein Verschoorstraat 31, NL-5611 SH Eindhoven (NL). **DEN HARTOG, Jos** [NL/NL]; Marienwaard 27, NL-2904 SE Capelle aan de Ijssel (NL).

(74) Agent: **MERTENS, H.V.**; Exter Polak & Charlouis B.V., P.O. Box 3241, NL-2280 GE Rijswijk (NL).

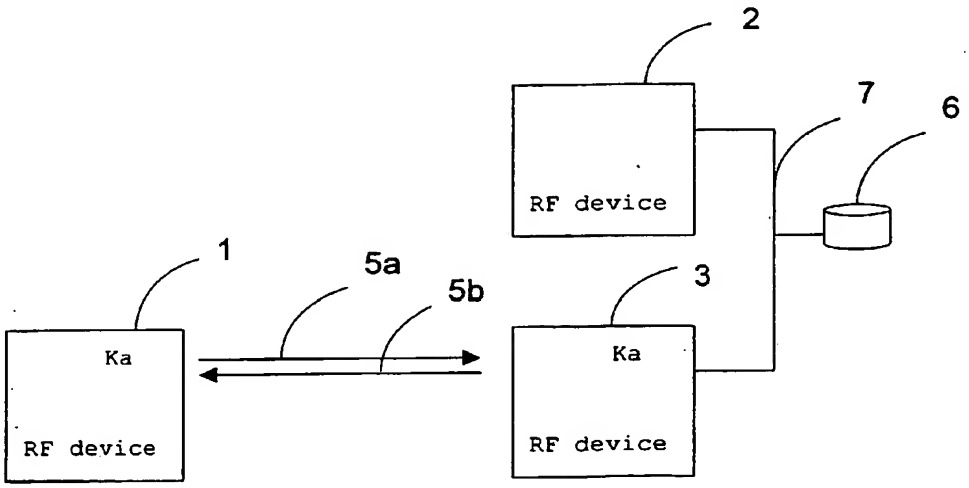
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: METHOD FOR ESTABLISHING CONNECTIONS BETWEEN RF DEVICES AND SYSTEM COMPRISING SUCH RF DEVICES



(57) Abstract: A method for establishing a connection between a first RF (Radio Frequency) device and a second RF device and a connection between the first RF device and a third RF device, the method comprising the steps of initialising the connection between the first device and the second device, paring the first device to the second device in a pairing procedure, resulting in a link key (ka) being known to the first device and to the second device. Further, establishing a subsequent connection between the first device and the third device comprises the steps of establishing a linking information comprising the link key (Ka) and an initial linking identity, initialising the connection between the first device and the third device, and assigning in the first device, based on the initial linking identity, the link key (Ka), being for exchanging messages between the first device and the third device.

WO 03/056746 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Method for establishing connections between RF devices and system comprising such RF devices

The invention relates to a method for establishing a connection between a first RF (Radio Frequency) device and a second RF device and a subsequent connection between the first RF device and a third RF device, the method comprising the steps of initialising the connection between the first device and the second device, pairing the first device to the second device in a pairing procedure, the pairing procedure resulting in a link key being known to the first device and to the second device, the link key being for exchanging messages between the first device and the second device. Further, the invention relates to a system comprising a first RF device and a group of RF devices.

The Specification of the Bluetooth System, Bluetooth Special Interest Group, version 1.0B, volumes 1 and 2, december 1999, describes a method for establishing a connection between devices. The specification of the Bluetooth system describes a layered structure of protocols which are involved in connections between RF devices. The layers include a baseband layer which determines an air interface, master and slave roles for devices, frequency hopping sequences and others. Further, the layers include a radio layer which includes radio- and frequency related items. Further, the layers include a linkmanager layer which includes bandwidth allocation and bandwidth reservation. Also, the link manager makes use of a challenge-response approach for authentication of devices. Further, link manager supervises pairing, being a creation of a trust relationship between two devices by generating and storing an authentication key for future device authentication. Also, the link manager supervises encryption of the data which is sent over the air interface, when needed. In the following, initializing a connection between two devices refers to all actions and protocols which are involved in setting up a connection, up to but excluding a pairing procedure. The pairing procedure is performed by a pair of devices for generating a link key in both devices, which link key can be used for a secure connection between these devices, which link key is

stored in both devices and which can be recalled later when a following connection between these two devices is established. The pairing procedure comprises the steps of generating an initialization key, which initialization key is derived from the Bluetooth address, a PIN-code, the length of the PIN-code and a random number. The random number is sent from the first device to the second device, enabling generation of the initialization key in both devices. Next, an authentication is performed, in which the first device sends a random number (a challenge), to the second device, followed by calculating a result in the first device and the second device, making use of the random number, the initialization key and the address of the second device, and sending a message from the second device to the first device, the message comprising the result. Now, in the first device a comparison is performed to verify if the result calculated in the first device is identical to the result calculated by the second device and sent to the first device. Next, a combination key is generated which will be used as the link key. As described in the specification of the Bluetooth System, generation of the combination key involves several steps to be performed in the first device and several steps to be performed in the second device, and a message sent from the first device to the second device and a message sent from the second device to the first device, the steps finally resulting in calculation of an identical combination key in the first device as well as in the second device. Finally, again an authentication procedure is performed in which the first device sends a challenge, comprising a random number, to the second device, in which both devices calculate a result making use of the random number and of the combination key, in which a response is sent from the second device to the first device comprising the result, and in which in the first device the result calculated by the first device is compared with the result calculated by the second device and sent to the first device, thus enabling a verification of the link key generated. When the link key is known to the first device and the second device, during a following connection between these devices only the last step, being the authentication procedure is performed for verification of the link key.

A problem is that the pairing procedure, which involves entering PIN-codes for both devices involved in the pairing

procedure, needs to be performed for each combination of devices separately. Thus, when setting up connections from a device to a plurality of devices such as an infrastructure, a pairing procedure needs to be performed for the device with each device of the plurality of devices. Consequently, PIN-codes have to be entered during each pairing procedure. Thus, this results in a user unfriendly situation, as a user has to enter a PIN-code every time the device of the user encounters a different Bluetooth device within the same infrastructure or the plurality of devices.

A second problem is that each link key needs to be stored for future use in the devices. Thus, a significant amount of storage capacity is required in the device for enabling communication with the plurality of devices or infrastructure, in particular if the infrastructure comprises a large number of devices.

The invention intends to simplify the pairing procedure for a device with a plurality of devices which form part of a group of devices.

To achieve this goal, the method according to the invention is characterized in that establishing the connection between the first device and the third device comprises the steps of establishing a linking information associating the first device to a group of devices comprising the second and third devices, the linking information comprising the link key and an initial linking identity, initialising the connection between the first device and the third device, sending the initial linking identity from the third device to the first device, sending the link key to the third device, and assigning in the first device, based on the initial linking identity, the link key, being for exchanging messages between the first device and the third device. The linking information, comprising the link key and the initial linking identity enables establishing a connection between the first device and the third device in a simple manner. After pairing of the first device with the second device, a link key is available to both these devices. According to the invention, when a subsequent connection between the first device and the third device has been initialized, the initial linking identity is sent from the third device to the first device, thus enabling the first device to recognize that no new pairing procedure with the third device is required. The link key, which has been determined

previously as a combination key in the pairing procedure between the first device and the second device, is sent (for example from the second device) to the third device, and in the first device the same link key which has already been determined during the pairing procedure between the first device and the second device is applied for the connection between the first device and the third device, in response to the initial linking identity sent from the third device to the first device. As a result, the link key, which has previously been determined during a pairing procedure between the first device and the second device, is now assigned for a connection between the first device and the third device, thus a pairing procedure between the first device and the third device is not required. The steps can be performed in the order shown, however it is also possible that the step of establishing a linking information is performed after the step of initializing the connection between the first device and the third device. Further, the step of sending the link key to the third device can be performed before or after any of the other steps for establishing the connection between the first device and the third device as described above.

Advantageously, the method comprises the further step of performing an authentication procedure by the first device with the third device, making use of the link key, after sending the initial linking identity from the third device to the first device. In this way it is possible for the first device to perform an authentication procedure with the third device, in a manner similar or identical to the authentication procedure performed by a device when setting up a link with an other device, the devices having performed a pairing procedure and consequently a link key for the connection between the two devices being known. Thus, a verification of the link key can be performed by an authentication procedure which can be identical to a known authentication procedure.

Advantageously, the step of establishing the linking information associating the first device to the group of devices comprises the step of storing the linking information in a database which is comprised in a network interconnecting the group of devices. The group of devices, which comprises the second and third device can be mutually connected via a network, such as a wired network or a wireless network, and a database can be comprised in the network.

Thus, the linking information comprising the link key and the initial linking identity can be stored in a database, allowing the devices which are comprised in the group of devices to have access to the linking information when required. Alternatively it is possible that the linking information is stored in a device of the group of devices, such as the second device, and when an other device of the group of devices requires access to the linking information or part of this information, it is sent to such other device.

Advantageously, the initial linking identity comprises an identity of the second device. Consequently, when the connection between the first device and the third device is or has been initialized, the third device sends the identity of the second device to the first device, causing the first device to make use of the link key already known as the first device has already paired with the second device. This makes it possible to simplify the first device, as in the first device only one entry is required, being an identity of the second device and the link key determined in the pairing procedure with the second device. As all other devices of the group now identify themselves towards the first device making use of the identity of the second device, no further link keys, and no further corresponding entries of identities of devices in a memory in the first device are required. Thus, the first device is able to establish connections with all devices in the group of devices while requiring storing of only a single link key for establishing connections with all devices of the group of devices. The identity of the second device can for example be an address of the second device.

Alternatively, the initial linking identity can comprise a group identification. Consequently, the third device sends a group identification to the first device. The first device, based on the group identification, assigns the link key already determined in the pairing procedure between the first device and the second device, to the connection between the first device and the third device. To accomplish this, at least the group identification and the link key are stored in or available to the first device. Thus, the first device assigns the link key previously determined in the pairing procedure between the first device and the second device to the connection with the third device as the group identification sent

from the third device to the first device identifies the third device as belonging to the same group as the second device.

Advantageously, the group identification is known to the first device by, before establishing the connection between the first device and the third device, sending the group identification from the second device to the first device, and storing the group identification in the first device. Thus, the group identification is sent to the first device in connection to the pairing procedure between the first device and the second device, enabling the first device to store the group identification in association with the link key determined.

Advantageously the group identification is stored in the first device in a table, enabling storage of one or more group identifications, corresponding link keys, and possibly identities of individual devices belonging to the group in the first device in a structured manner.

Further, the invention comprises a system comprising a first RF device and a group of RF devices comprising at least a second and a third device, enabling the first device to establish connections with at least one device of the group of devices, making use of the method according to the invention.

Advantageously, the devices of the group of devices are connected via a network to each other and to a database, the database comprising a memory for storing the linking information. Thus, each device of the group of devices has access to the linking information, when required, via the network. The linking information can be stored in the memory comprised in the database, allowing the devices of the group of devices to have convenient access to the linking information. Further, remote maintenance is facilitated, as, in case that a link key of a device, such as the first device needs to be removed, this can simply be performed by updating the linking information in the database.

Advantageously, the network comprises a wired network. Alternatively, it is of course possible that the devices comprised in the group of devices exchange information and transfer messages to each other via a wireless connection.

Further advantages and features of the invention will become clear from the appended drawing, showing a non-limiting embodiment, in which:

Fig. 1a-1d highly schematically shows a pairing procedure according to the state of the art and

Fig. 2a and 2c highly schematically illustrate the method according to the invention.

Fig. 1a shows a generation of an initialization key K_{init}. The initialization key K_{init} is generated by entering a PIN-code in the first device 1 as well as the second device 2. Further, in the first device 1 a random number IN_RAND_a is generated and sent to the second device 2. Now, both devices calculate the initialization key K_{init} from the random number IN_RAND_a, the PIN-code and an address BD_ADDR_b of the second device. Next, Fig. 1b shows a verification procedure in which the first device 1 sends a challenge, being a random number AU_RAND_a to the second device 2, both devices calculate a result SRES and the second device 2 sends the result SRES back to the first device 1. The first device 1 now compares the results SRES, and if these are equal, the pairing procedure proceeds from this authentication step to the next step depicted in Fig. 1c. In this next step, the link key Ka is calculated in both the first device 1 and the second device 2. A number Ca is generated in the first device 1 and sent to the second device 2, and a number Cb is generated in the second device 2 and sent to the first device 1. The number Ca is generated in the first device 1 from a random number LK_RAND_a and the initialization K_{init}, and in the second device 2 the number Cb is generated from the initialization key K_{init} and a random number LK_RAND_b. Then, making use of the initialization key K_{init}, in the first device 1 the random number LK_RAND_b, which has been generated in the second device 2, and in the second device, the random number LK_RAND_a which has been generated in the first device, are recovered. Now, in the first device 1 as well as in the second device 2, a combination key which will be used as the link key Ka is generated from the random number LK_RAND_a and LK_RAND_b, as well as from the addresses of the first device 1 and the second device 2, BD_ADDR_a and BD_ADDR_b. Finally an authentication procedure is performed, similar to the challenge response procedure described in Fig. 1b, in which a verification is performed if the link key Ka calculated in the first

device 1 and the second device 2 is identical. Then, the link key Ka is stored in the first device 1 and the second device 2 and can be recalled later for future connections between the first device 1 and the second device 2.

Fig. 2a shows a first device 1, a second device 2 and a third device 3. The first device 1 initializes a connection (indicated by arrows 4a, 4b) with- and performs a pairing procedure with the second device 2. The second device 2 and the third device 3 both belong to an infrastructure, such as a public infrastructure. According to the invention, as shown in Fig. 2c a subsequent pairing procedure of the first device 1 with the third device 3 is not required. The first device 1, which has, as depicted in Fig. 2a, paired with the second device 2 can easily and conveniently set up a connection with the third device 3. After the pairing procedure of the first device 1 with the second device 2, which includes the steps shown in Fig. 1a-1d, the first device 1 and the second device 2 both have a link key Ka (being the combination key) available for a connection 4a,4b between the first device 1 and the second device 2, as depicted in Fig. 2b.

When the first device 1 initializes a connection 5a,5b with the third device 3, as depicted in Fig. 2c, after having established a connection 4a,4b with the second device 2, as depicted in Figs. 2a and 2b, pairing is not required, as the link key Ka (being the combination key) which has been determined by the first device 1 and the second device 2 in the pairing procedure according to Fig. 2a, will be used also for a subsequent connection 5a, 5b between the first device 1 and the third device 3. To accomplish this, an initial linking identity is sent from the third device 3 to the first device 1. This initial linking identity can for example comprise an address of the second device 2, which is sent by the third device 3 to the first device 1. Upon receipt of the initial linking identity, comprising e.g. the address of the second device 2, the first device 1 assigns the link key Ka which is already known and assigned to the connection or any subsequent connection between the first device 1 and the second devise 2, to the connection 5a, 5b between the first device 1 and the third device 3, in response to the address of the second device 2 which has been sent by the third device 3. The link key Ka, which is determined in the second device 2 in the pairing

procedure according to Fig. 2a, can either be sent by the second device 2 to the third device 3, however it is also possible that the link key Ka is sent from the second device 2 to a database 6 and stored in a memory in the database 6. From the database 6, the link key Ka is sent to the third device 3. Now, both the first device 1 and the third device 3 have the link key Ka available and associated to the connection between these devices, implying that the need for a pairing procedure between the first device and the third device 3 has disappeared. Thus, after following a pairing procedure between the first device 1 and the second device 2 according to Fig. 2a, a linking information is established which associates the first device 1 to a group of devices comprising the second device 2 and the third device 3. The linking information comprises the link key Ka and the initial linking identity. The linking information can be stored in a memory in the database 6, however it is also possible that the linking information is kept available in the second device 2, making a separate database, such as the database 6 for storing linking information superfluous Instead of the initial linking identity comprising an address, it is also possible that the initial linking identity comprises a group identification. In this case, the group of devices comprising the second device 2 and the third device 3 is identified by a group identification, which group identification is sent to the first device 1. Based on the group identification, the first device 1 now assigns the link key Ka to the connection between the first device 1 and the third device 3. The group identification can be transferred to the first device 1 during the pairing procedure between the first device 1 and the second device 2 according to Fig. 2a, and can be stored in the first device 1 in association with the link key Ka. Thus, when the connection with an other device which belongs to the same group as device 2 is established by the first device 1, the sending of the group identification by that device which forms part of the group of devices, is recognized by the first device 1, and because of the association between the group identification and the link key Ka the link key Ka issued for the communication between the first device 1 and the device which belongs to the group of devices. When, as depicted in Fig. 2c, the first device 1 and the third device 3 both have the link key Ka assigned to the connection between these devices, an authentication procedure,

similar to the authentication procedure, depicted in Fig. 1d can be performed, thus performing a verification to check if the link key Ka in the two devices is identical.

The connection 7 between the second device 2 and the third device 3, and between the devices 2, 3 forming part of the group of devices and the database 6 can be a wired connection, such as a telecommunication network or a data communication network. Alternatively, it is possible that the connection between the devices 2, 3 which are comprised in the group of devices comprises a wireless network, which can comprise connections between devices in the group of devices similar or identical to the connections between the first and the second, respectively the third device, resulting in a simple implementation.

Sending an identity of the second device 2, comprised in the initial linking identity from the third device 3 to the first device 1 has the advantage that is does require little or no modifications in the first device 1. Also, the amount of memory required in the first device 1 for storing different link keys as well as addresses of devices belonging to the group of devices is low, as only the link key Ka and the address of the second device 2 (or any other device of the group of devices with which the first device 1 has initially performed a pairing procedure) needs to be stored in the first device 1. In this case, the linking information comprises the address of the second device 2 (or any other address of the particular device with which the first device 1 has initially performed a pairing procedure) which address or other identity of that device belonging to the group of devices is stored either in one or more of the devices 2, 3 of the group of devices, and/or in the database 6. If the initial linking identity comprises a group identification, then the first device 1 needs to be arranged for storing the group identification such that the group identification associated to the link key Ka is stored, for example in a table comprising link keys, group identifications and possibly identities (such as addresses) of individual devices.

Consequently, the invention allows "network level pairing", thus allows a device to perform a pairing procedure with a device which forms part of a group (or network) of devices by means of a single pairing procedure between the device and one of the devices of

the group of devices. Subsequent pairing procedures with other devices of the group of devices are not required, and thus the need for determining link keys and need for entering PIN-codes when the device establishes a first connection with any of the other devices which form part of the group of devices is not required; as the link key determined in the pairing procedure between the device and one of the group of devices is used for any other subsequent connection between the device and any device of the group of devices.

The devices can for example be Bluetooth devices and the connections be Bluetooth connections complying to the specification of the Bluetooth system referenced in this document. According to the invention, a Bluetooth device, obtaining access to a network or group of Bluetooth devices, only needs to perform a single pairing procedure with one of the devices of the group (or network) of devices and from that moment on the device is able to establish connections and exchange messages with all devices belonging to the group (or network) of devices making use of the link key determined in the single pairing procedure. Other wireless connections making use of other RF technologies are however also possible.

Advantages of the invention will become apparent particularly in case that the group of devices is a Bluetooth infrastructure, such as a public Bluetooth infrastructure, in which case a subscriber device (a device of a user) only needs to perform a single pairing procedure, comprising entering of a PIN-code in order to be able to establish connections with all devices belonging to the group of devices which form part of the Bluetooth infrastructure after having performed the pairing procedure with one of the devices which forms part of the infrastructure. Thus, a user-friendly procedure has been created as repeated entering of PIN-codes is not required. Further, storing of a large number of link keys, i.e. an individual link key for a connection of the device with each one of the devices of the infrastructure with which a communication has been set up, is not required.

CLAIMS

1. Method for establishing a connection between a first RF (Radio Frequency) device (1) and a second RF device (2) and a subsequent connection between the first RF device (1) and a third RF (3) device, the method comprising the steps of
- initialising the connection between the first device (1) and the second device (2);
- pairing the first device (1) to the second device (2) in a pairing procedure, the pairing procedure resulting in a link key (Ka) being known to the first device (1) and to the second device (2), the link key (Ka) being for exchanging messages between the first device (1)and the second device (2),
the method being characterised in that establishing the connection between the first device (1) and the third device (3) comprises the steps of:
- establishing a linking information associating the first device (1) to a group of devices comprising the second (2) and third (3)devices, the linking information comprising the link key (Ka) and an initial linking identity;
- initialising the connection between the first device (1)and the third device (3);
- sending the initial linking identity from the third device (3) to the first device (1);
- sending the link key (Ka) to the third device (3); and
- assigning in the first device (1), based on the initial linking identity, the link key (Ka), being for exchanging messages between the first device (1) and the third device (3).

2. The method according to claim 1, characterised by the further step of performing an authentication procedure by the first device (1) with the third device (3), making use of the link key (Ka), after sending the initial linking identity from the third device (3) to the first device (1).

3. The method according to claim 1 or 2, characterised in that the step of establishing the linking information associating the first device (1) to the group of devices (2,3) comprises the step of

storing the linking information in a database (6) which is comprised in a network (7) interconnecting the group of devices (2,3).

4. The method according to any of claims 1 - 3, characterised in that the initial linking identity comprises an identity of the second device (2).

5. The method according to any of claims 1 - 3, characterised in that the initial linking identity comprises a group identification.

6. The method according to claim 5, characterised by the further steps of before establishing the connection between the first device (1)and the third device (3):
- sending the group identification from the second device (2)to the first device (1); and
- storing the group identification in the first device (1).

7. The method according to claim 6, characterised in that the step of storing the group identification in the first device (1) comprises the step of storing the group identification in the first device (1) in a table.

8. A system comprising a first RF device (1) and a group of RF devices comprising at least a second (2)and a third (3) device, enabling the first device (1)to establish connections with at least one device (3)of the group of the devices (2,3) making use of the method according to any of the preceding claims.

9. The system according to claim 8, characterised in that the devices of the group of devices (2,3) are connected via a network (7) to each other and to a database (6), the database comprising a memory for storing the linking information.

10. The system according to claim 9, characterised in that the network (7)comprises a wired network.

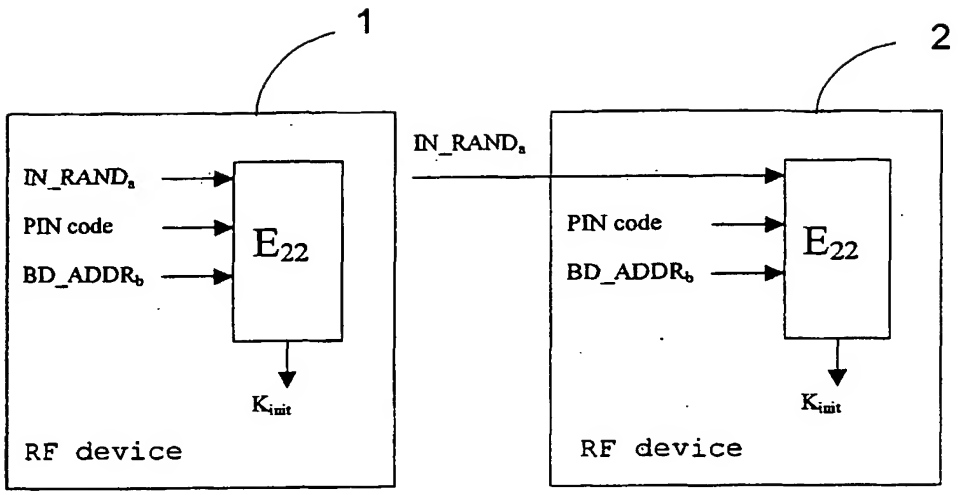

1
2
IN_RAND$_a$
PIN code
BD_ADDR$_b$
E_{22}
K_{init}
RF device
IN_RAND$_a$
PIN code
BD_ADDR$_b$
E_{22}
K_{init}
RF device

Fig. 1a

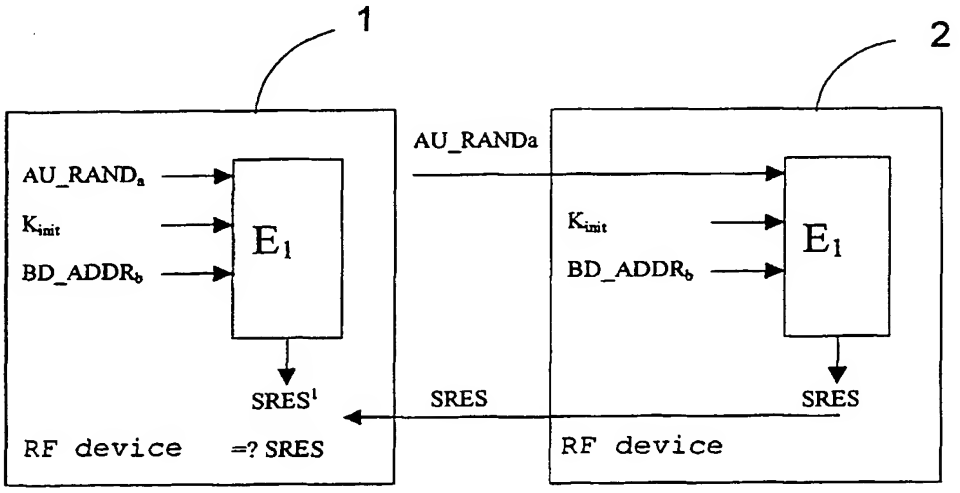

1
2
AU_RAND$_a$
K_{init}
BD_ADDR$_b$
E_1
$SRES^1$
RF device =? SRES
AU_RANDa
K_{init}
BD_ADDR$_b$
E_1
SRES
SRES
RF device

Fig. 1b

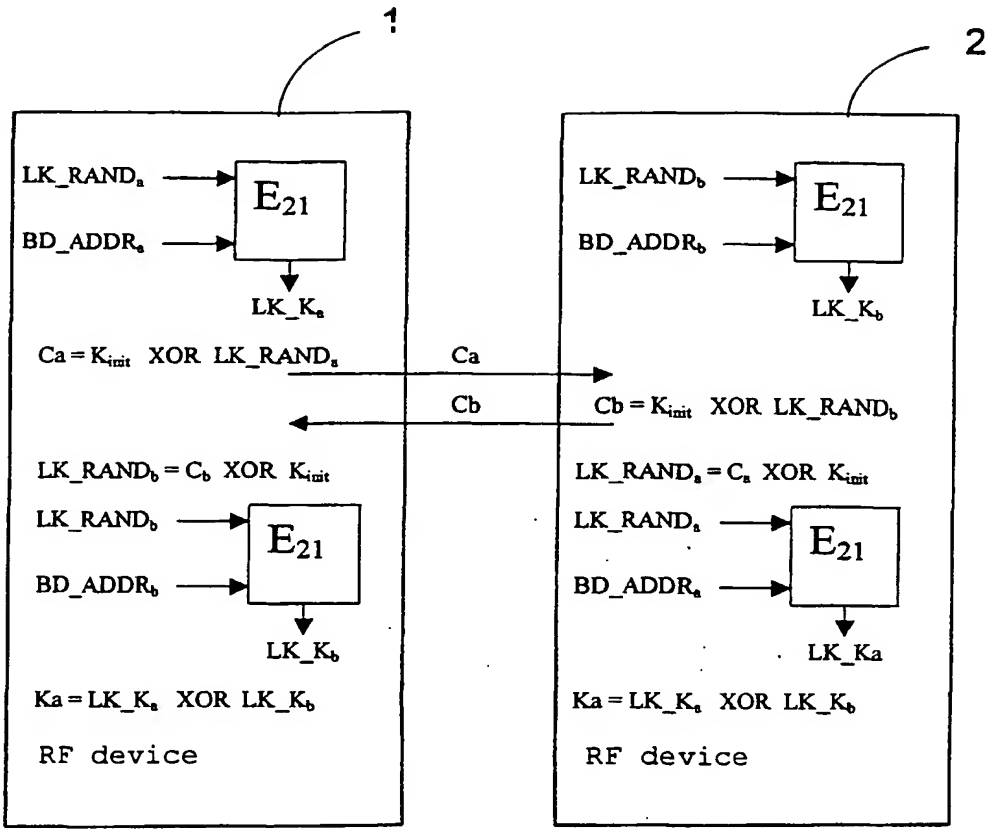

1
2
LK_RAND$_a$
BD_ADDR$_a$
E_{21}
LK_K$_a$
Ca = K$_{init}$ XOR LK_RAND$_a$
Ca
Cb
Cb = K$_{init}$ XOR LK_RAND$_b$
LK_RAND$_b$ = C$_b$ XOR K$_{init}$
LK_RAND$_b$
BD_ADDR$_b$
E_{21}
LK_K$_b$
Ka = LK_K$_a$ XOR LK_K$_b$
RF device
LK_RAND$_b$
BD_ADDR$_b$
E_{21}
LK_K$_b$
LK_RAND$_a$ = C$_a$ XOR K$_{init}$
LK_RAND$_a$
BD_ADDR$_a$
E_{21}
LK_Ka
Ka = LK_K$_a$ XOR LK_K$_b$
RF device

Fig. 1c

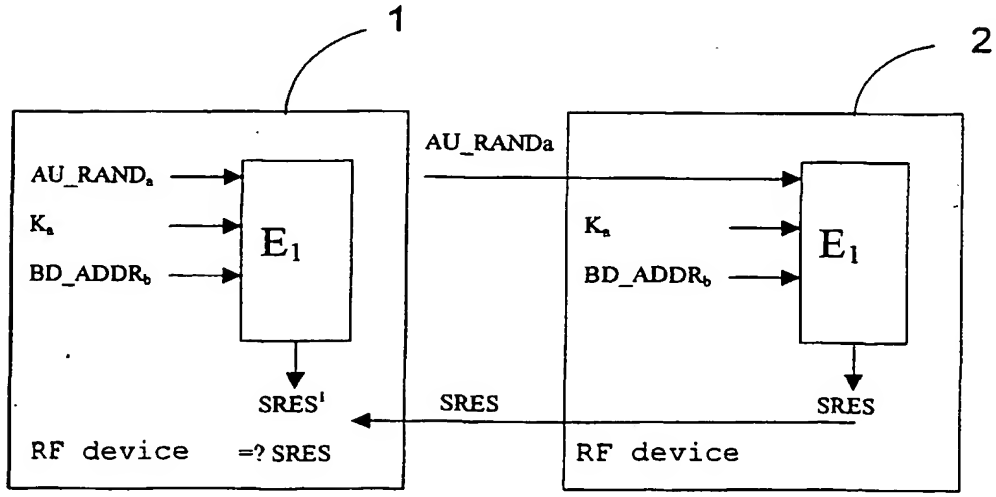

1
2
AU_RANDa
AU_RAND$_a$
K$_a$
BD_ADDR$_b$
E_1
SRES'
RF device =? SRES
SRES
K$_a$
BD_ADDR$_b$
E_1
SRES
RF device

Fig. 1d

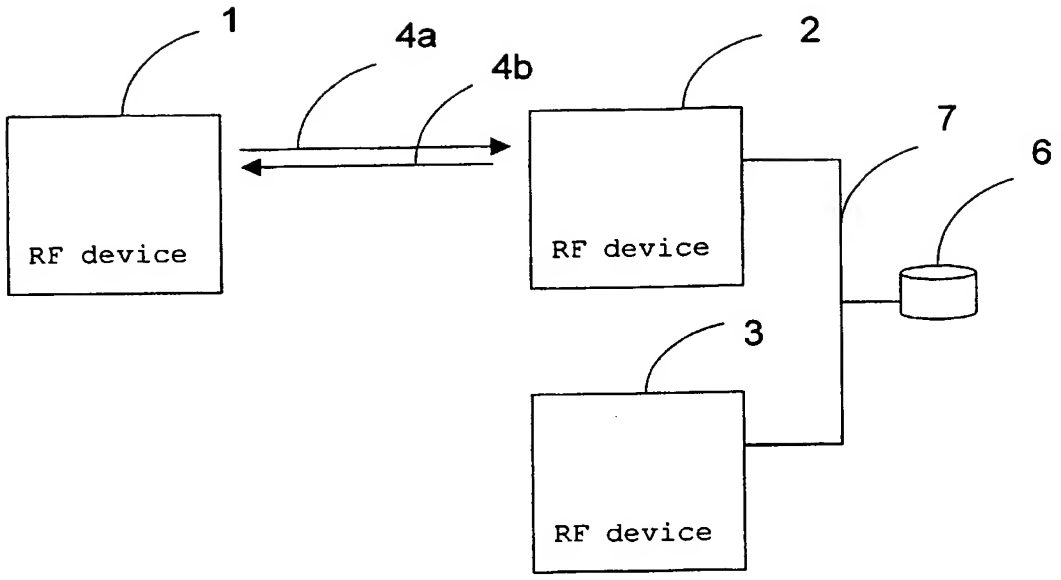

1
4a
4b
2
7
6
RF device
RF device
3
RF device

Fig. 2a

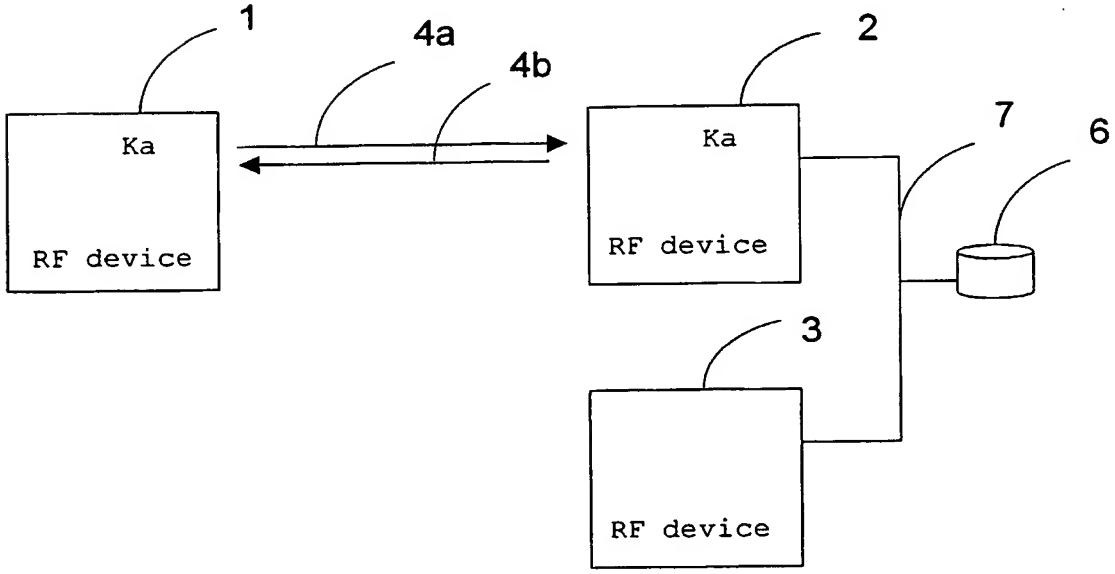

1
4a
4b
2
7
6
Ka
RF device
Ka
RF device
3
RF device

Fig. 2b

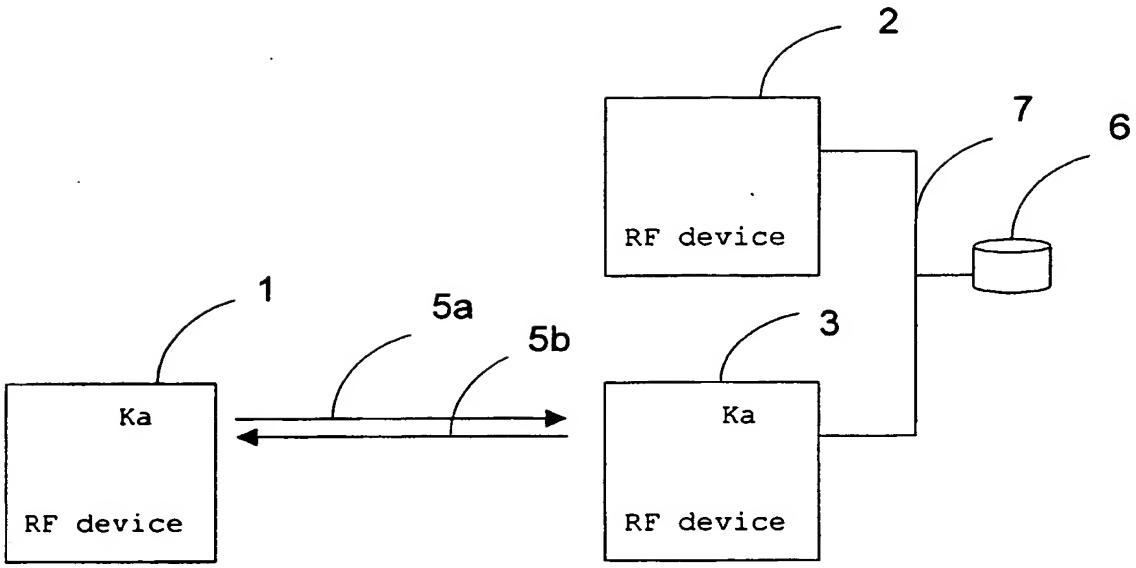


Fig. 2c

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 02/00057

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	"SPECIFICATION OF THE BLUETOOTH SYSTEM version 1.0 B" SPECIFICATION OF THE BLUETOOTH SYSTEM, 1 December 1999 (1999-12-01), XP002175286 cited in the application paragraph '14.2.2.2! - paragraph '14.2.2.8! paragraph '14.4! - paragraph '14.5.4! ---	1-10
A	WO 00 76120 A (NOKIA MOBILE PHONES LTD.) 14 December 2000 (2000-12-14) abstract; figures 7A-11 page 14, line 23 -page 15, line 30 --- -/--	1

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 September 2002	30/09/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Danielidis, S

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 02/00057

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ASOKAN N ET AL: "Key agreement in ad hoc networks" COMPUTER COMMUNICATIONS, ELSEVIER SCIENCE PUBLISHERS BV, AMSTERDAM, NL, vol. 23, no. 17, 1 November 2000 (2000-11-01), pages 1627-1637, XP004238466 ISSN: 0140-3664 the whole document	1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 02/00057

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0076120 A	14-12-2000	GB 2350971 A	13-12-2000
		AU 5401200 A	28-12-2000
		BR 0010416 A	13-02-2002
		CN 1354947 T	19-06-2002
		WO 0076120 A2	14-12-2000
		EP 1188290 A2	20-03-2002